4. Learn definitions and types of vulnerabilities.

Definitions and Types of Vulnerabilities

1. What is a Vulnerability?

A **vulnerability** is a flaw, weakness, or misconfiguration in software, hardware, or network systems that can be exploited by an attacker to compromise security.

- **Key Impact Areas:**

- **Confidentiality** – Data exposure.
- **Integrity** – Unauthorized data modification.
- **Availability** – Disruption of services (DoS attacks).

---

2. Types of Vulnerabilities

A. Software Vulnerabilities

These are coding flaws that allow attackers to manipulate software behavior.

- **Examples:**

1. **Buffer Overflow** – Writing more data than a buffer can hold, leading to arbitrary code execution.
2. **SQL Injection (SQLi)** – Injecting SQL commands to access or modify a database.
3. **Cross-Site Scripting (XSS)** – Injecting malicious scripts into web pages to steal user data.
4. **Remote Code Execution (RCE)** – Running attacker-controlled code remotely.
5. **Integer Overflow** – Exploiting numerical limits to manipulate program logic.

B. System Misconfiguration Vulnerabilities

These occur due to insecure settings or improper system setup.

- **Examples:**

1. **Default Credentials** – Leaving default usernames/passwords unchanged.
2. **Unpatched Software** – Running outdated applications vulnerable to known exploits.
3. **Exposed Services** – Leaving unnecessary ports open (e.g., SSH, RDP, SMB).
4. **Weak Permissions** – Overly permissive file access (`chmod 777`).
5. **Misconfigured Firewalls** – Allowing unauthorized traffic or excessive exposure.

C. Network Vulnerabilities

Weaknesses in network design, implementation, or encryption protocols.

- **Examples:**

1. **Man-in-the-Middle (MITM)** – Intercepting and altering communication between parties.
2. **Denial of Service (DoS)** – Overloading a system to make it unavailable.
3. **DNS Spoofing** – Redirecting users to malicious websites.
4. **Weak Encryption** – Using outdated encryption like **MD5** or **WEP**.
5. **ARP Poisoning** – Manipulating Address Resolution Protocol (ARP) tables to redirect traffic.

D. Human-Related Vulnerabilities

Exploiting human mistakes or lack of security awareness.

- **Examples:**

1. **Social Engineering** – Tricking people into revealing sensitive information.
2. **Phishing Attacks** – Fake emails tricking users into providing credentials.
3. **Shoulder Surfing** – Observing someone's screen or keyboard inputs.
4. **Weak Passwords** – Using easily guessable passwords (`123456`, `password`).
5. **Insider Threats** – Employees leaking or misusing sensitive data.

---

3. Vulnerability Severity Classification

- **Common Vulnerability Scoring System (CVSS)** – Assigns a **0-10** severity score:

Score	Severity
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

- **Other Scoring Methods:**

- **DREAD Model** (Damage, Reproducibility, Exploitability, Affected Users, Discoverability).
- **STRIDE Model** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).

---

4. Real-World Example of a Vulnerability

- **CVE-2021-44228 (Log4Shell)** – A critical **Remote Code Execution (RCE)** vulnerability in Log4j.
- **CVSS Score: 10.0 (Critical)**
- **Impact:** Attackers could execute arbitrary code remotely on affected systems.

Conclusion

Vulnerabilities can exist in **software, system configurations, networks, and human behavior**. Understanding their types and classification helps in securing systems against **exploits** and **cyberattacks**.